Performance of Entanglement-assisted Quantum LDPC Codes Constructed From Finite Geometries

Min-Hsiu Hsieh
ERATO-SORST Quantum Computation and Information Project, Japan Science and Technology Agency 5-28-3, Hongo, Bunkyo-ku, Tokyo, Japan

Wen-Tai Yen, and Li-Yi Hsu
Department of Physics, Chung Yuan Christian University, Chungli, Taiwan
(Date textdate)

We investigate the performance of entanglement-assisted quantum low-density parity-check (LDPC) codes constructed from finite geometries. Though the entanglement-assisted formalism provides a universal connection between a classical linear quaternary code and an entanglement-assisted quantum error-correcting code (EAQECC), the issue of maintaining large amount of pure maximally entangled states in constructing EAQECCs is a practical obstacle to its use. We provide families of EAQECCs with an entanglement consumption rate that decreases exponentially. Surprisingly, these EAQECCs outperform those codes constructed in [1].

PACS numbers: PACS number
Keywords: Low density parity check codes, Euclidean geometry, projective geometry, cyclic code, quasi-cyclic code

I. INTRODUCTION

The goal of coding theory is to design families of codes with transmission rate approaching the channel capacity [2], while the error probability of the transmitted message is arbitrarily small. Practical encoding and decoding implementation is also desirable. Originally, Shannon employed nonconstructive random codes with no practical encoding and decoding algorithm. It is not surprising that most of the families of the constructed codes so far do not satisfy both of the requirements. Exceptions are the low-density parity-check (LDPC) codes [3] and Turbo codes [4].

The LDPC code was first proposed in 1963 [3] that was much earlier than the formation of modern coding theory. Not until the early 90's, the LDPC code was rediscovered as family of sparse codes [5], and was shown to have capacity-approaching performance while the complexity of implementing encoding and decoding algorithms is relatively low. A (J, L)-regular LDPC code is defined to be the null space of a binary parity check matrix H with the following properties: (1) each column consists of J "ones"; (2) each row consists of L "ones"; (3) both J and L are small compared to the length of the code n and the number of rows in H.

There are several methods of constructing good families of regular LDPC codes [5, 6, 7]. Among them, the LDPC codes that are constructed from finite geometry have the following advantages: (1) they have good minimum distance; (2) the girth of these codes is at least 6; (3) they perform very well with iterative decoding, only a few tenths of a dB away from the Shannon theoretical limit; (4) they can be put into either cyclic or quasi-cyclic form. Consequently, their encoding can be achieved in linear time and implemented with a single feedback shift register; (5) they can be extended or shortened in various ways to obtain other good LDPC codes [6].

The connection between classical linear codes and the quantum codes is unified by the entanglement-assisted coding theory [8, 9]. Every classical linear code can be used to construct the corresponding quantum code with the help of a certain amount of pre-shared entanglement. When the classical code is self-dual, the resulting EAQECC is equivalent to a stabilizer code [10]. Furthermore, the entanglement-assisted formalism preserves the minimum distance property of the classical code—large minimum distance classical code results in en entanglement-assisted quantum error-correcting code (EAQECC) with the same minimum distance.

Large minimum distance of a code (both quantum or classical) might not directly link to its error probability performance [11]. The error probability performance also largely depends on the decoding algorithms [6]. Classically, the sum-product decoding (belief propagation decoding) algorithm [12] provides good trade-off between the error probability and the code's decoding complexity. It is natural to consider a quantum generalization of the sum-product algorithm even though the *degeneracy* property of a quantum code is not fully addressed in such a generalization [13].

In this paper, we construct families of EAQECCs from two types of finite geometries: the Euclidean geometry and the projective geometry. Moreover, we show that the pre-shared entanglement required to construct some codes decreases exponentially with respect to the length of the code. We evaluate their block error probability performance over the depolarizing channel when decoding with the sum-product decoding algorithm. Their block error probability performance is better than the codes proposed in [1].

This paper is organized as follows. In Section II, we first introduce the Euclidean geometry and the projective

geometry. Then, we discuss several properties of these two finite geometries and show how to construct classical finite geometric LDPC (FG-LDPC) codes. In Section III, we construct EAQECCs from classical FG-LDPC codes. Specifically, we construct several EAQECCs that require an arbitrarily small amount of entanglement. In Section IV, we compare the performance of the EAQECCs constructed from classical FG-LDPC codes with the known results in the literature. In section V, we concludes.

II. FINITE GEOMETRY AND FINITE GEOMETRY LDPC CODES

In this section, we give definitions of finite geometries and show how to construct classical FG-LDPC codes. Ref. [6] contains an excellent introduction of the Euclidean and projective geometries.

A finite geometry $\mathbf{G}$ with n points and m lines is said to have the following fundamental structural properties: (1) every line consists of L points; (2) any two points are connected by one and only one line; (3) Every point is intersected by J lines; (4) two lines are either parallel or they intersect at one and only one point. There are two families of finite geometries which have the above properties, the Euclidean and projective geometries over finite fields.

A. Euclidean geometry

Let $\mathrm{EG}(p,q)$ be a p-dimensional Euclidean geometry over the Galois field $\mathrm{GF}(q)$ where p and q are two positive integers. This geometry consists of q^p points, and each point can be represented by a p-tuple over $\mathrm{GF}(q)$. The all-zero p-tuple $\mathbf{0} = (0, 0, \cdots, 0)$ is called the origin. In other words, all the points in $\mathrm{EG}(p,q)$ form a p-dimensional vector space over $\mathrm{GF}(q)$. A line in $\mathrm{EG}(p,q)$ can be viewed as a one-dimensional subspace of $\mathrm{EG}(p,q)$ or a coset of it. Therefore, a line in $\mathrm{EG}(p,q)$ consists of q points. Furthermore, the Euclidean geometry has the following properties: (1) there are $q^{p-1}(q^p-1)/(q-1)$ lines; (2) for any point in $\mathrm{EG}(p,q)$, there are $(q^p-1)/(q-1)$ lines intersecting it; (3) every line has $q^{p-1}-1$ lines parallel to it.

1. Type-I EG-LDPC

To show how to construct a binary parity check matrix using the Euclidean geometry, we need a few definitions. Let $\mathrm{GF}(q^p)$ be the *extension field* of $\mathrm{GF}(q)$. Then every point in $\mathrm{EG}(p,q)$ is an element of the Galois field $\mathrm{GF}(q^p)$, henceforth $\mathrm{GF}(q^p)$ can be regarded as the Euclidean geometry $\mathrm{EG}(p,q)$. Let α be a primitive element of $\mathrm{GF}(q^p)$. Then $0, 1, \alpha, \alpha^2, \cdots, \alpha^{q^p-2}$ can be mapped to each of the q^p points in $\mathrm{EG}(p,q)$.

Let $\mathbf{H}^{(1)}_{\mathrm{EG}(p,q)}$ be the binary matrix whose rows are the incidence vectors of all the lines in $\mathrm{EG}(p,q)$ that do not pass through the origin and whose columns are the q^p-1 non-origin points. The columns are arranged in the order of $1, \alpha, \alpha^2, \cdots, \alpha^{q^p-2}$, i.e., the $(i+1)$-th column corresponds to the point α^i. Then $\mathbf{H}^{(1)}_{\mathrm{EG}(p,q)}$ has $n = q^p-1$ columns and $m = (q^{p-1}-1)(q^p-1)/(q-1)$ rows. To sum up, the binary matrix $\mathbf{H}^{(1)}_{\mathrm{EG}(p,q)}$ has the following structural properties: (1) each row has weight $L = q$. This correspondence results from each line of $\mathrm{EG}(p,q)$ containing q points; (2) each column has weight $J = (q^p-1)/(q-1)-1$. This correspondence results from the fact that each point has $(q^p-1)/(q-1)$ lines intersecting at this point, but one of them passes through the origin; (3) any two columns have at most one nonzero element in common; (4) any two rows have at most one nonzero element in common; (5) the density of $\mathbf{H}^{(1)}_{\mathrm{EG}(p,q)}$ is

$$\frac{L}{n} = \frac{J}{m} = \frac{q}{q^p-1}.$$

We can make the density smaller by picking larger p and q; (6) The minimum distance of the code defined by $\mathbf{H}^{(1)}_{\mathrm{EG}(p,q)}$ is $J+1$. This can be proved using the BCH-bound [14].

To be more specific, suppose ℓ is a line not passing through $\mathbf{0}$. We can define the incidence vector of ℓ (the ℓ-th row in $\mathbf{H}^{(1)}_{\mathrm{EG}(p,q)}$) as

$$\mathbf{v}_\ell = (v_1, v_2, \cdots, v_n),$$

where $v_i = 1$ if the point α^i lies in the line ℓ, otherwise $v_i = 0$. Clearly, $\alpha^k\ell$ is also a line in $\mathrm{EG}(p,q)$, for $k = 0, 1, n-1$, and $\alpha\mathbf{v}_\ell$ is a right cyclic-shift of $\mathbf{v}_\ell$.

Consider the respective incidence vectors of lines ℓ_j, $\alpha\ell_j, \cdots, \alpha^{n-1}\ell_j$. We can construct a binary $n \times n$ matrix H_j from them as follows:

$$H_j \equiv \begin{pmatrix} \mathbf{v}_{\ell_j} \\ \mathbf{v}_{\alpha\ell_j} \\ \vdots \\ \mathbf{v}_{\alpha^{n-1}\ell_j} \end{pmatrix}. \tag{1}$$

Here H_j is a circulant matrix with column and row weights equal to q. Since the total number of lines in $\mathrm{EG}(p,q)$ not passing through $\mathbf{0}$ is $(q^p-1)(q^{p-1}-1)/(q-1)$, we can partition these lines into $(q^{p-1}-1)/(q-1)$ cyclic classes (each cyclic class is represented by a binary $n \times n$ cyclic matrix H_j). Finally, we can construct $\mathbf{H}^{(1)}_{\mathrm{EG}(p,q)}$ by

$$\mathbf{H}^{(1)}_{\mathrm{EG}(p,q)} = \begin{pmatrix} H_1 \\ H_2 \\ \vdots \\ H_{\frac{q^{p-1}-1}{q-1}} \end{pmatrix}. \tag{2}$$

The null space of $\mathbf{H}^{(1)}_{\mathrm{EG}(p,q)}$ is a type-I EG-LDPC code. Furthermore, type-I EG-LDPC codes are cyclic codes.

2. Type-II EG-LDPC

The type-II EG-LDPC is obtained by taking the transpose of $\mathbf{H}^{(1)}_{\mathrm{EG}(p,q)}$:

$$\mathbf{H}^{(2)}_{\mathrm{EG}(p,q)} \equiv \left(\mathbf{H}^{(1)}_{\mathrm{EG}(p,q)}\right)^T = \left(\begin{array}{cccc} H_1^T & H_2^T & \cdots & H_{\frac{q^{p-1}-1}{q-1}}^T \end{array} \right).$$

The null space of $\mathbf{H}^{(2)}_{\mathrm{EG}(p,q)}$ is a type-II EG-LDPC code. Clearly, type-II EG-LDPC codes are quasi-cyclic codes.

The binary matrix $\mathbf{H}^{(2)}_{\mathrm{EG}(p,q)}$ has the following structural properties: (1) each column has weight $J = q$; (2) each row has weight $L = (q^p-1)/(q-1)-1$; (3) any two columns have at most one nonzero element in common; (4) any two rows have at most one nonzero element in common; (5) the density of $\mathbf{H}^{(2)}_{\mathrm{EG}(p,q)}$ is

$$\frac{L}{n} = \frac{J}{m} = \frac{q}{q^p-1};$$

(6) the minimum distance of the code defined by $\mathbf{H}^{(2)}_{\mathrm{EG}(p,q)}$ is $J+1$.

B. Projective geometry

Let $\mathrm{GF}(q^{p+1})$ be the *extension field* of $\mathrm{GF}(q)$, and let α be a primitive element of $\mathrm{GF}(q^{p+1})$. Let $n = (q^{p+1}-1)/(q-1)$, and $\beta = \alpha^n$. Then the order of β is $q-1$, and $\{0, 1, \beta, \cdots, \beta^{q-2}\}$ form all elements of $\mathrm{GF}(q)$. Consider the set $\{\alpha^0, \alpha^1, \cdots, \alpha^n\}$, and partition the nonzero elements of $\mathrm{GF}(q^{p+1})$ into n disjoint subsets as follows:

$$(\alpha^j) = \{\alpha^j, \beta\alpha^j, \cdots, \beta^{q-2}\alpha^j\},$$

for $j = 0, 1, \cdots, n-1$. Therefore, for any $\alpha^i \in \mathrm{GF}(q^{p+1})$, if $\alpha^i = \beta^\ell \alpha^j$ with $0 \le j < n$, then α^i is in the set (α^j).

If we represent each element in $\mathrm{GF}(q^{p+1})$ as an $(p+1)$-tuple over $\mathrm{GF}(q)$, then (α^j) consists of $q-1$ $(p+1)$-tuples over $\mathrm{GF}(q)$.

Define $\mathrm{PG}(p,q)$ to be a p-dimensional projective geometry over $\mathrm{GF}(q)$. This geometry consists of $n = (q^{p+1}-1)/(q-1)$ points, and each point is represented by (α^j), for $0 \le j < n$. In other words, these $q-1$ elements, $\{\alpha^j, \beta\alpha^j, \cdots, \beta^{q-2}\alpha^j\}$, of $\mathrm{GF}(q^{p+1})$ is considered as the same point in $\mathrm{PG}(p,q)$. Therefore, these points, $(\alpha^0), (\alpha^1), \cdots, (\alpha^n)$, form a p-dimensional projective geometry over $\mathrm{GF}(q)$. Note that a projective geometry does not have a origin. The projective geometry has the following properties: (1) each line in $\mathrm{PG}(p,q)$ consists of $q+1$ points; (2) the number of lines in $\mathrm{PG}(p,q)$ that intersect at a given point is $(q^p-1)/(q-1)$; (3) there are

$$\frac{(1+q+\cdots+q^{p-1})(1+q+\cdots+q^p)}{q+1}$$

lines in $\mathrm{PG}(p,q)$.

1. Type-I PG-LDPC

Let $\mathbf{H}^{(1)}_{\mathrm{PG}(p,q)}$ be the binary matrix whose rows are the incidence vectors of all lines in $\mathrm{PG}(p,q)$ and whose columns are the all the points of $\mathrm{PG}(p,q)$. The columns are arranged in the following order: $(\alpha^0), (\alpha), \cdots, (\alpha^{n-1})$. Then $\mathbf{H}^{(1)}_{\mathrm{PG}(p,q)}$ has $n = (q^{p+1}-1)/(q-1)$ columns and $m = (1+q+\cdots+q^{p-1})(1+q+\cdots+q^p)/(q+1)$ rows. To sum up, the binary matrix $\mathbf{H}^{(1)}_{\mathrm{PG}(p,q)}$ has the following structural properties: (1) each row has weight $L = q+1$. This correspondence results from each line in $\mathrm{PG}(p,q)$ containing $q+1$ points; (2) each column has weight $J = (q^p-1)/(q-1)$. This correspondence results from the fact that each point has $(q^p-1)/(q-1)$ lines intersecting at this points; (3) any two columns have at most one nonzero element in common; (4) any two rows have at most one nonzero element in common; (5) the density of $\mathbf{H}^{(1)}_{\mathrm{PG}(p,q)}$ is

$$\frac{L}{n} = \frac{J}{m} = \frac{q^2-1}{q^{p+1}-1}.$$

We can make the density smaller by picking $p \ge 2$; (6) the minimum distance of the code defined by $\mathbf{H}^{(1)}_{\mathrm{PG}(p,q)}$ is $J+1$. This can be proved using BCH-bound [14]. Similar to the type-I EG-LDPC, the type-I PG-LDPC code is also cyclic.

2. Type-II PG-LDPC

The type-II PG-LDPC is obtained by taking the transpose of $\mathbf{H}^{(1)}_{\mathrm{PG}(p,q)}$:

$$\mathbf{H}^{(2)}_{\mathrm{PG}(p,q)} \equiv \left(\mathbf{H}^{(1)}_{\mathrm{PG}(p,q)}\right)^T \tag{3}$$

The null space of $\mathbf{H}^{(2)}_{\mathrm{PG}(p,q)}$ is called the type-II PG-LDPC code. Clearly, type-II PG-LDPC codes are quasi-cyclic codes.

The binary matrix $\mathbf{H}^{(2)}_{\mathrm{PG}(p,q)}$ has the following structural properties: (1) each column has weight $J = q+1$; (2) each row has weight $L = \frac{q^p-1}{q-1}$; (3) any two columns have at most one nonzero element in common; (4) any two rows have at most one nonzero element in common; (5) the density of $\mathbf{H}^{(2)}_{\mathrm{PG}(p,q)}$ is

$$\frac{L}{n} = \frac{J}{m} = \frac{q^2-1}{q^{p+1}-1};$$

(6) the minimum distance of the code defined by $\mathbf{H}^{(2)}_{\mathrm{PG}(p,q)}$ is $J+1$.

III. ENTANGLEMENT-ASSISTED QUANTUM FINITE GEOMETRY LDPC CODES

Recall that the girth of the classical FG-LDPC codes is at least 6 due to the geometric structure of finite geometry [6]. This makes the construction of dual-containing quantum LDPC codes impossible because the classical FG-LDPC codes do not contain their dual unless necessary modification of the original classical FG-LDPC codes is made [15, 16].

The authors in Ref. [8, 17] proposed the entanglement-assisted stabilizer formalism that includes the standard quantum error-correcting codes as a special case. The entanglement-assisted stabilizer formalism generalizes the stabilizer theory of quantum error correction. If the CSS construction for quantum codes is applied to a classical code which is not dual-containing, the resulting "stabilizer" group is not commuting, and thus has no code space. With entanglement shared between sender and receiver before quantum communication begins, this noncommuting stabilizer group can be embedded in a larger space, which makes the group commute, and allows a code space to be defined. This construction can be applied to any classical linear quaternary code, not just dual-containing ones. The existing theory of quantum error correcting codes thus becomes a special case of the entanglement-assisted stabilizer theory: dual-containing classical codes give rise to standard quantum codes, while non-dual containing classical codes give rise to entanglement-assisted quantum error correction codes.

The following theorem regards the amount of maximally entangled states (ebits) required in the construction of EAQECCs from arbitrary classical binary codes [18, 19, 20].

Theorem 1 *Let H be any binary parity check matrix with dimension $(n-k)\times n$. We can obtain the corresponding $[[n, 2k-n+e; e]]$ EAQECC, where $e = \mathrm{rank}(HH^T)$ is the number of ebits needed.*

Noiseless entanglement is a valuable resource, and protecting it from the environment might require extra error-correcting power. Therefore, it is desirable to use as small amount of entanglement in EAQECCs as possible. Theorem 1 provides a general guideline for evaluating the amount of entanglement required; however, no concrete steps of constructing EAQECCs with small amount of entanglement were proposed there.

Define the *entanglement consumption rate* of an $[[n, k; e]]$ EAQECC to be e/n. Previously, evidence indicates that the amount of entanglement in the entanglement-assisted quasi-cyclic LDPC codes might increase linearly with the code length [1]. Here, we illustrate three families of EAQECCs constructed from classical FG-LDPC codes such that the entanglement consumption rate decreases when the code length increases.

The first example follows from classical type-I 2-dimensional EG-LDPC codes over Euclidean geometry $\mathrm{EG}(2, 2^s)$. Such type-I 2-D EG-LDPC code is an $[n, k, d]$ linear code where $n = 2^{2s} - 1$, $n - k = 3^s - 1$, and $d = 2^s + 1$. Furthermore, the parity check matrix $\mathbf{H}^{(1)}_{\mathrm{EG}(2,2^s)}$ has both row weight L and column weight J equal to 2^s [6].

Theorem 2 *The rank of $\mathbf{H}^{(1)}_{\mathrm{EG}(2,2^s)}(\mathbf{H}^{(1)}_{\mathrm{EG}(2,2^s)})^T$ is equal to 2^s.*

Proof. Denote $\overline{\mathrm{EG}}(2, 2^s)$ to be the Euclidean geometry $\mathrm{EG}(2, 2^s)$ where both the origin and the lines passing through it are excluded. Then $\overline{\mathrm{EG}}(2, 2^s)$ contains $2^{2s} - 1$ points and $2^{2s} - 1$ lines. Recall the definition of a line in Euclidean geometry $\mathrm{EG}(2, 2^s)$ from Section II. Any line in $\overline{\mathrm{EG}}(2, 2^s)$ induces a partition of $\overline{\mathrm{EG}}(2, 2^s)$ into $2^s + 1$ sets, where each set S_i, $i = 1, 2, \cdots, 2^s+1$, contains lines parallel to each other. It is also easy to verify that the size of each S_i is $2^s - 1$. We consider the following three cases:

1. Recall that the number of points on a line is 2^s. Therefore, the overlapping of the number of "ones" in the incidence vector with itself is even, and the inner product of an incidence vector with itself is zero.

2. Since two different lines in the same set are parallel to each other, the overlapping of the number of "ones" in these two incidence vectors is zero. The inner product of these two incidence vectors is zero.

3. Since two arbitrary different lines in two different sets intersect at only one point, the overlapping of the number of "ones" in these two incidence vectors is one. The inner product of these two incidence vectors is one.

Since the rows of $\mathbf{H}^{(1)}_{\mathrm{EG}(2,2^s)}$ come from all the incidence vectors of those lines in $\overline{\mathrm{EG}}(2, 2^s)$, we can arrange the rows in the order of the lines in S_i, where i starts from 1 to 2^s+1. Then the matrix $\mathbf{H}^{(1)}_{\mathrm{EG}(2,2^s)}(\mathbf{H}^{(1)}_{\mathrm{EG}(2,2^s)})^T$ consists of $(2^s + 1) \times (2^s + 1)$ submatrices:

$$\begin{pmatrix} \mathbf{0} & \mathbf{1} & \cdots & \mathbf{1} \\ \mathbf{1} & \mathbf{0} & & \mathbf{1} \\ \vdots & & \ddots & \vdots \\ \mathbf{1} & \cdots & & \mathbf{0} \end{pmatrix},$$

where each $\mathbf{0}$ or $\mathbf{1}$ represents an all-zeros or all-ones matrix of size $(2^s - 1) \times (2^s - 1)$, respectively. The rank of $\mathbf{H}^{(1)}_{\mathrm{EG}(2,2^s)}(\mathbf{H}^{(1)}_{\mathrm{EG}(2,2^s)})^T$ is then equal to 2^s. ■

Table I lists a set of $[[n, 2k-n+e, d; e]]$ EAQECCs [8, 17] constructed from the classical type-I 2-D EG-LDPC code whose parity check matrix $\mathbf{H}^{(1)}_{\mathrm{EG}(2,2^s)}$ has row weight L and column weight J. The entanglement consumption rate in this case is

$$\frac{e}{n} = \frac{2^s}{2^{2s} - 1}, \tag{4}$$

s	n	k	d	L	J	e
2	15	7	5	4	4	4
3	63	37	9	8	8	8
4	255	175	17	16	16	16
5	1023	781	33	32	32	32
6	4095	3367	65	64	64	64
7	16383	14197	129	128	128	128

TABLE I: Each row represents an $[[n, 2k-n+e, d; e]]$ EAQECC, respectively, that is constructed from the classical type-I 2-D EG-LDPC code whose parity check matrix $\mathbf{H}^{(1)}_{\mathrm{EG}(2,2^s)}$ has row weight L and column weight J.

s	n	k	d	L	J	e
2	21	11	6	5	5	1
3	73	45	10	9	9	1
4	273	191	18	17	17	1
5	1057	813	34	33	33	1
6	4161	3431	66	65	66	1
7	16513	14326	130	129	129	1

TABLE II: Each row represents an $[[n, 2k-n+e, d; e]]$ EAQECC, respectively, that is constructed from the classical type-I 2-D PG-LDPC code whose parity check matrix $\mathbf{H}^{(1)}_{\mathrm{PG}(2,2^s)}$ has row weight L and column weight J.

which decreases exponentially as s increases.

The second example follows from classical type-I 2-dimensional PG-LDPC codes over projective geometry $\mathrm{PG}(2, 2^s)$. Such type-I 2-D PG-LDPC code is an $[n, k, d]$ linear code where $n = 2^{2s} + 2^s + 1$, $n - k = 3^s - 1$, and $d = 2^s + 2$. Furthermore, the parity check matrix $\mathbf{H}^{(1)}_{\mathrm{EG}(2,2^s)}$ has both row weight L and column weight J equal to $2^s + 1$ [6].

Theorem 3 *The rank of* $\mathbf{H}^{(1)}_{\mathrm{PG}(2,2^s)}(\mathbf{H}^{(1)}_{\mathrm{PG}(2,2^s)})^T$ *is equal to* 1, $\forall s \in \mathbb{Z}^+$.

Proof. Recall that $\mathrm{PG}(2, 2^s)$ contains $2^{2s} + 2^s + 1$ points and $2^{2s} + 2^s + 1$ lines, and every line intersects with another one at exactly one point. The overlapping of the number of "ones" in these two incidence vectors is one. Therefore, the inner product of these two incidence vectors is one. Furthermore, the number of points on a line is $2^s + 1$, the overlapping of the number of "ones" in the incidence vector with itself is odd. The inner product of the incidence vector with itself is one.

Since the rows of $\mathbf{H}^{(1)}_{\mathrm{PG}(2,2^s)}$ come from all the incidence vectors of those lines in $\mathrm{PG}(2, 2^s)$, the matrix $\mathbf{H}^{(1)}_{\mathrm{PG}(2,2^s)}(\mathbf{H}^{(1)}_{\mathrm{PG}(2,2^s)})^T$ is an all-one matrix. The rank of $\mathbf{H}^{(1)}_{\mathrm{PG}(2,2^s)}(\mathbf{H}^{(1)}_{\mathrm{PG}(2,2^s)})^T$ is then equal to 1. ■

Table II lists a set of $[[n, 2k-n+e, d; e]]$ EAQECCs constructed from the classical type-I 2-D PG-LDPC code whose parity check matrix $\mathbf{H}^{(1)}_{\mathrm{PG}(2,2^s)}$ has row weight L and column weight J. The entanglement consumption rate in this case is

$$\frac{e}{n} = \frac{1}{2^{2s} + 2^s + 1}, \tag{5}$$

which decreases exponentially as s increases.

The third example follows from classical type-II 3-dimensional PG-LDPC codes over projective geometry $\mathrm{PG}(3, q)$.

Theorem 4 *The rank of* $\mathbf{H}^{(2)}_{\mathrm{PG}(3,q)}(\mathbf{H}^{(2)}_{\mathrm{PG}(3,q)})^T$ *is equal to* 1, *for every integer* $q \geq 2$.

Proof. Here, we consider a 3-dimensional projective geometry over $\mathrm{GF}(q)$. Recall that each line in $\mathrm{PG}(3, q)$ contains $L = q^2 + q + 1$ points, where L is odd for $q \geq 2$. Therefore, the inner product of the row vector with itself is one. Furthermore, two different points are connected by exactly one line. Therefore, the overlapping of the number of "ones" in arbitrary two rows is one. The inner product of these two incidence vectors is one. Therefore the matrix $\mathbf{H}^{(2)}_{\mathrm{PG}(3,q)}(\mathbf{H}^{(2)}_{\mathrm{PG}(3,q)})^T$ is an all-one matrix. The rank of $\mathbf{H}^{(2)}_{\mathrm{PG}(3,q)}(\mathbf{H}^{(2)}_{\mathrm{PG}(3,q)})^T$ is then equal to 1. ■

Table III lists a set of $[[n, 2k-n, d; e]]$ EAQECCs constructed from the classical type-II 3-D PG-LDPC code whose parity check matrix $\mathbf{H}^{(2)}_{\mathrm{PG}(3,q)}$ has row weigh L and column weigh J. Again the construction uses the "generalized CSS construction" proposed in Ref. [8, 17]. The entanglement consumption rate in this case is

$$\frac{e}{n} = \frac{q+1}{(1+q+q^2)(1+q+q^2+q^3)}, \tag{6}$$

which decreases polynomially as q increases.

q	n	k	d	L	J	e
2	35	24	4	7	3	1
3	130	91	5	13	4	1
4	357	296	6	21	5	1
5	806	651	7	31	6	1
6	2850	2451	8	43	7	1
7	4745	4344	9	57	8	1

TABLE III: Each row represents an $[[n, 2k-n+e, d; e]]$ EAQECC, respectively, that is constructed from the classical type-II 3-D PG-LDPC code whose parity check matrix $\mathbf{H}^{(2)}_{\mathrm{PG}(3,q)}$ has row weight L and column weight J.

IV. PERFORMANCE

In this section, we provide simulation results (in terms of block error rate) of the quantum FG-LDPC codes over the depolarizing channel, which creates X errors, Y errors, and Z errors with equal probability f_m. Moreover, we focus on those quantum FG-LDPC codes with a low

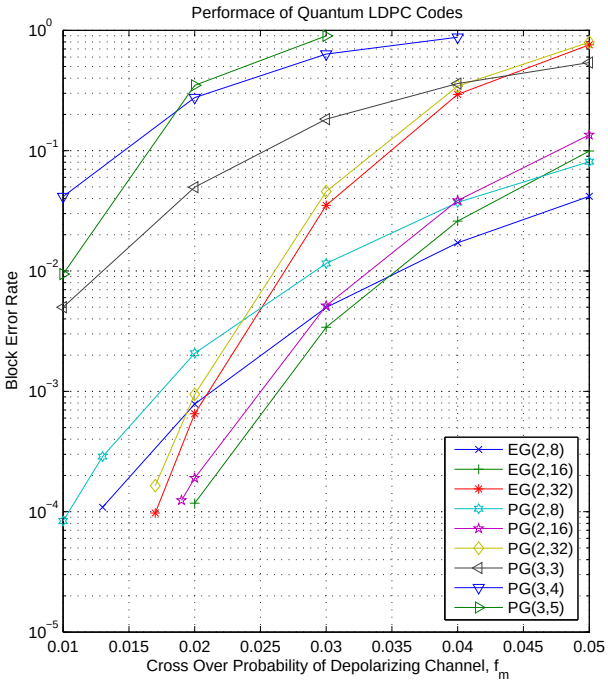

FIG. 1: (Color online). Block error probability performance of quantum FG-LDPC codes with SPA decoding, and 100 iterations for each date point.

entanglement consumption rate. The decoding algorithm used in the simulation is the sum-product decoding algorithm. For simplicity, we omit the introduction of this decoding algorithm, and point the interested reader to Refs. [5, 13].

Fig. 1 shows that the block error probability performance of EG(2,32) is better than EG(2,16), and the block error probability performance of EG(2,16) is better than EG(2,8) when the cross over probability f_m is small ($f_m < 0.015$). A similar result holds for quantum PG-LDPC codes. However, the block error probability performance for shorter code length is better when the cross error probability is large. The reason for this might be because in the quantum setting, the transmitted quantum information cannot be retrieved even when the whole block contains just one uncorrectable error. In this sense, using quantum code with large block might not be helpful, unlike in the classical setting.

The authors in [1] investigated the block error probability performance of entanglement-assisted quantum quasicyclic LDPC codes, and showed that their EAQECCs outperform some existing quantum stabilizer codes with similar *net rate*, where the net rate of an $[[n, k; e]]$ EAQECC is defined to be $(k - e)/n$. Surprisingly, the 2-D entanglement-assisted FG-LDPC codes perform much better than their constructed examples. Moreover, the consumed pure entanglement in constructing the entanglement-assisted FG-LDPC codes is much less than theirs.

Next, we modify the sum-product decoding algorithm according to the heuristic methods proposed in [13]. Those modifications are intended to overcome the ignorance of the degeneracy in the decoding. However, our simulation shows that those modifications do not help to improve any performance for decoding the entanglement-assisted FG-LDPC codes. For example, in Fig. 2, we show the performance of the SPA decoding with random perturbation (see Ref. [13] for further detail) is the same as that of no random perturbation for the EG(2,8) EAQECC. The reason for such result is because the degeneracy effect is mild. Those low weight errors are not likely to be inside the code space due to the large minimum distance property of the FG-LDPC codes.

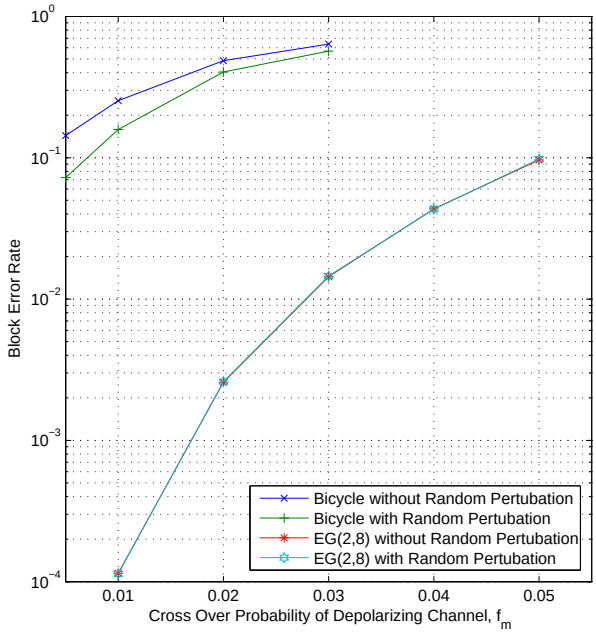

FIG. 2: (Color online). Performance of quantum FG-LDPC codes with modified SPA decoding. The stabilizer code constructed by the bicycle technique (see Ref. [11]) encodes 30 logical qubits in 60 physical qubits. The maximum number of iterations for its SPA decoding is 100, and the number of iterations between each perturbation is 6. The strength of the random perturbation is 0.1. The maximum number of iterations of the SPA decoding for the EG(2,8) EAQECC is 100, and the number of iterations between each perturbation is also 6.

V. CONCLUSION

In this paper, we construct families of EAQECCs from finite geometries such that the block error probability performance of these codes is relatively better than those proposed in the literature so far. The improvement

largely comes from lack of cycles of length 4 of the constructed FG-LDPC codes due to the geometric structure. Furthermore, we can overcome the problem of maintaining large amount of pure maximally entangled states in constructing EAQECCs by providing families of EAQECCs with an exponentially decreasing entanglement consumption rate.

The degeneracy effect of the entanglement-assisted FG-LDPC codes is mild because low weight errors are unlikely to be codewords due to the guaranteed large minimum distance of the FG-LDPC codes. Therefore, we do not need to modify the sum-product decoding algorithm which would largely increase the decoding complexity. However, we believe that new decoding technique that incorporates the coset construct of the quantum codes deserves further investigation.

Acknowledgments

The author MHH thanks Mark M. Wilde for his useful suggestions and comments on the draft. The authors LYH and YWT acknowledge support from National Science Council of the Republic of China under Contract No. NSC.96-2112-M-033-007-MY3.

[1] M. H. Hsieh, T. Brun, and I. Devetak. Entanglement-assisted quantum quasicyclic low-density parity-check codes. *Physical Review A*, 79:032340, 2009.

[2] C. E. Shannon. A mathematical theory of communication. *Bell System Tech. Jnl.*, 27:379–423, 623–656, 1948.

[3] R. G. Gallager. *Low-Density Parity-Check Codes*. PhD thesis, Massachusetts Institute of Technology, 1963.

[4] C. Berrou, A. Glavieux, and P. Thitimajshima. Near shannon limit error-correcting coding and decoding: Turbo codes. In *Proceedings of the IEEE International Communications Conference*, pages 1064–1070, 1993.

[5] D. J. C. MacKay. Good error-correcting codes based on very sparse matrices. *IEEE Transactions on Information Theory*, 45:399–432, 1999.

[6] Y. Kou, S. Lin, and M. Fossorier. Low-density parity-check codes based on finite geometries: A rediscovery and new results. *IEEE Transactions on Information Theory*, 47:2711–2736, 2001.

[7] M. Fossorier. Quasi-cyclic low-density parity-check codes from circulant permutation matrices. *IEEE Transactions on Information Theory*, 50(8):1788–1793, 2004.

[8] T. Brun, I. Devetak, and M. H. Hsieh. Correcting quantum errors with entanglement. *Science*, 314(5798):436–439, 2006.

[9] M. H. Hsieh. *Entanglement-assisted Coding Thoery*. PhD thesis, University of Southern California, Los Angeles, CA, 2008. in preparation.

[10] D. Gottesman. *Stabilizer codes and quantum error correction*. PhD thesis, California Institute of Technology, 1997.

[11] D. J. C. MacKay, G. Mitchison, and P. L. McFadden. Sparse-graph codes for quantum error correction. *IEEE Transactions on Information Theory*, 50:2315–2330, 2004.

[12] R. M. Tanner. A recursive approach to low complexity codes. *IEEE Transactions on Information Theory*, 27:533–547, 1981.

[13] David Poulin and Yeojin Chung. On the iterative decoding of sparse quantum codes. *Quantum Information and Computation*, 8(10):987–1000, 2008.

[14] W. W. Peterson and Jr. E. J. Weldon. *Error-Correcting Codes*. MIT Press, Cambridge, MA, 1972.

[15] Salah A. Aly. A class of quantum ldpc codes constructed from finite geometries, 2007. arXiv:0712.4115.

[16] Manabu Hagiwara and Hideki Imai. Quantum quasi-cyclic ldpc codes. *IEEE International Symposium on Information Theory (ISIT)*, 2007.

[17] T. Brun, I. Devetak, and M. H. Hsieh. Catalytic quantum error correction, 2006. quant-ph/0608027.

[18] M. H. Hsieh, I. Devetak, and T. Brun. General entanglement-assisted quantum error-correcting codes. *Physical Review A*, 76:062313, 2007.

[19] Mark M. Wilde and Todd A. Brun. Optimal entanglement formulas for entanglement-assisted quantum coding. *Physical Review A*, 77:064302, 2008.

[20] Mark M. Wilde. Logical operators of quantum codes. *Physical Review A*, 79:062322, 2009.